Read Only Domain Controller – Vorbereiten & Bereitstellen

Inhalt

Read Only Domain Controller - Einleitung 2
Read Only Domain Controller - Vorbereitung 3
Read Only Domain Controller - Bereitstellen 10

Read Only Domain Controller - Einleitung

Mit dem Read Only Domain Controller (kurz RODC), hat Microsoft ein neues und sehr nützliches Features in die Server 2008 Technologie gepackt.

Read Only Domain Controller - bietet den Administrator eine Lösung an, die immer wieder vor dem gleichen Problem in den Zweigstellen stehen. Entweder haben sie derzeit keinen Domänencontroller vor Ort und die Benutzer klagen über Verbindungsprobleme oder aber es ist ein schreibbaren Domain Controller vor Ort, aber dafür kann der Administrator keine physische Sicherheit gewährleiten bzw. fehlt die erforderliche Netzwerk Bandbreite um diesen anständig betreiben zu können.

Die folgenden Eigenschaften von RODCs ermöglichen die Lösung dieser Probleme:

- Schreibgeschützte Active Directory-Datenbank (NTDS.dit)
- Attributsatz mit RODC-Filter
- Unidirektionale Replikation
- Zwischenspeicherung von Anmeldeinformationen
- Aufteilung der Administratorrolle
- DNS ohne Schreibzugriff

Quellen:

Microsoft:

http://technet.microsoft.com/de-de/library/cc755058%28WS.10%29.aspx

http://technet.microsoft.com/de-de/library/cc753223%28WS.10%29.aspx

http://technet.microsoft.com/de-de/library/cc753348%28WS.10%29.aspx

Yusufs.Directory.Blog:

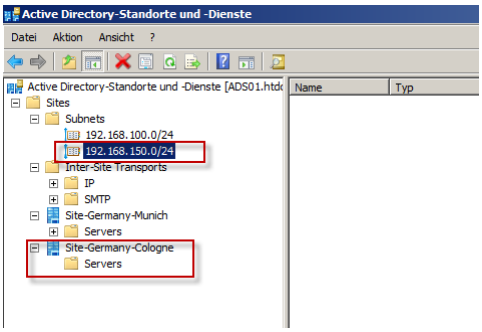
http://blog.dikmenoglu.de/ReadOnly+Domain+Controller+RODC.aspx

Read Only Domain Controller - Vorbereitung

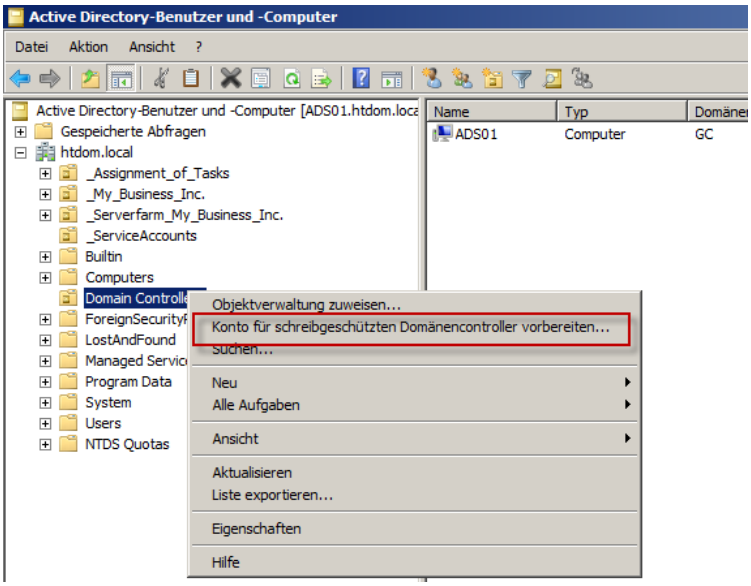
Szenario: - Wir haben einen neuen Außenstandort in Köln bekommen, um den Vertrieb in Deutschland ein bisschen auf Vordermann zu bringen, in diesen Standort fangen drei neue Mitarbeiter an und alle sind nur Anwender. ☺ Derzeit stellen die drei Mitarbeiter per VPN einen Connect in unser Netzwerk her, die Telefongesellschaft kann aber derzeit nur eine Maximale Bandbreite von 768 Kbit/s liefern, da das Büro doch sehr weit weg vom Schuss ist und ein Business Connect wäre für den Anfang einfach ein bisschen zu teuer. Man weiß ja nie was passiert. ☺

Daher entscheiden wir uns in München für einen Read Only Domain Controller um den Mitarbeitern zum einen ein bisschen Entlastung zu geben bezüglich der Einwahl und zum zweiten die klagen und Support Tickets zu minimieren.

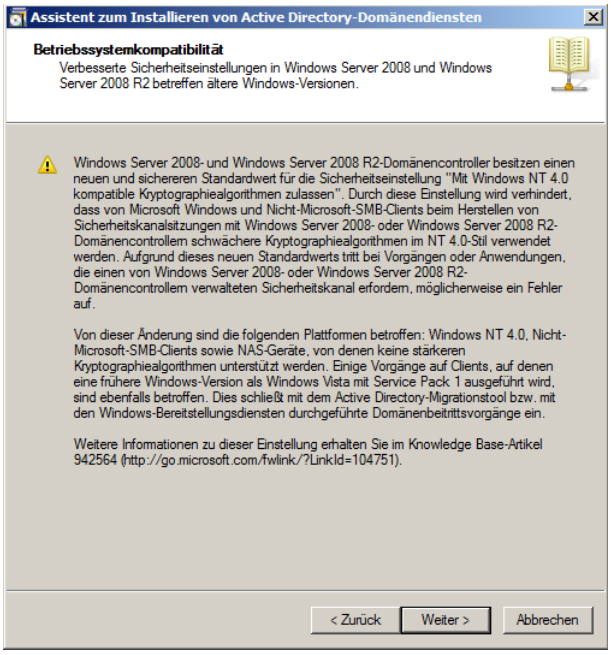
Um nun den RODC vorzubereiten öffnen wir in München die Active Directory-Standort und Dienste Verwaltung, legen dort einen neuen Standort an mit dem passenden Subnetz.



Als nächstes öffnen wir die Active Directory Benutzer und Computer Verwaltung und klicken auf die ***OU Domain Controller*** mit der rechten Maustaste im Kontextmenü wählen wir den Punkt „***Konto für den Schreibgeschützten Domaincontroller vorbereiten***“

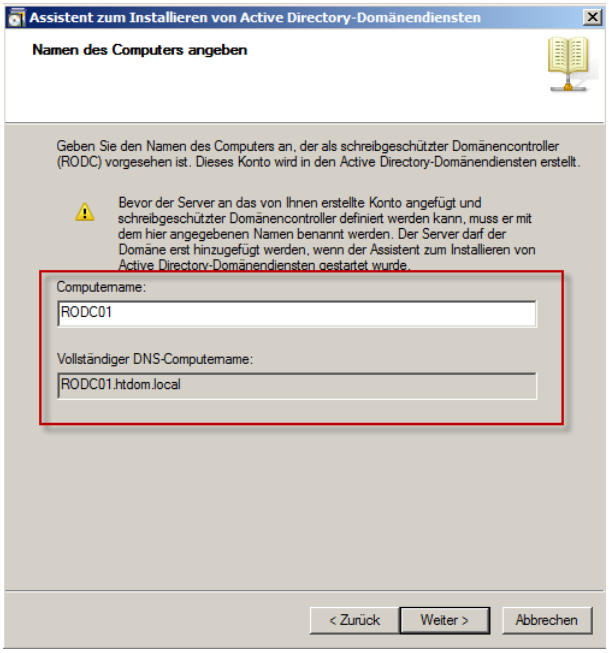


Es startet ein Einrichtungs- Wizard für den RODC, hier klicken den erweiterten Modus an und anschließend auf Weiter.

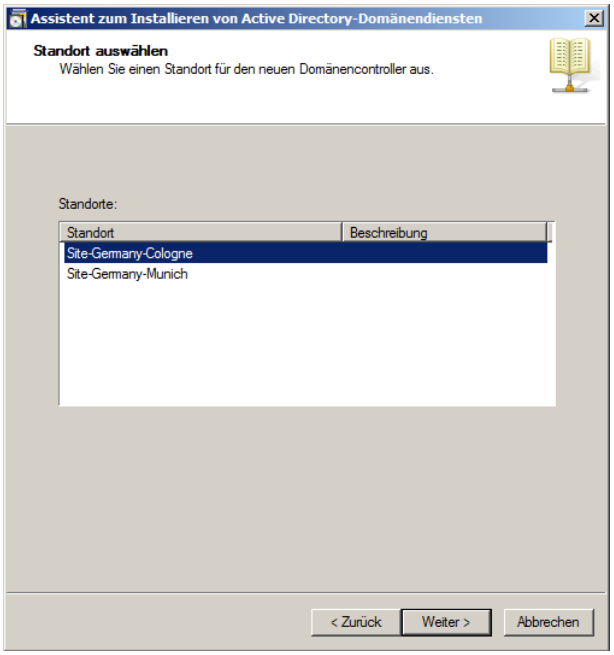


Das Fenster mit der Betriebssystemkompatibilität lesen wir uns durch und bestätigen das Ganze mit Weiter.

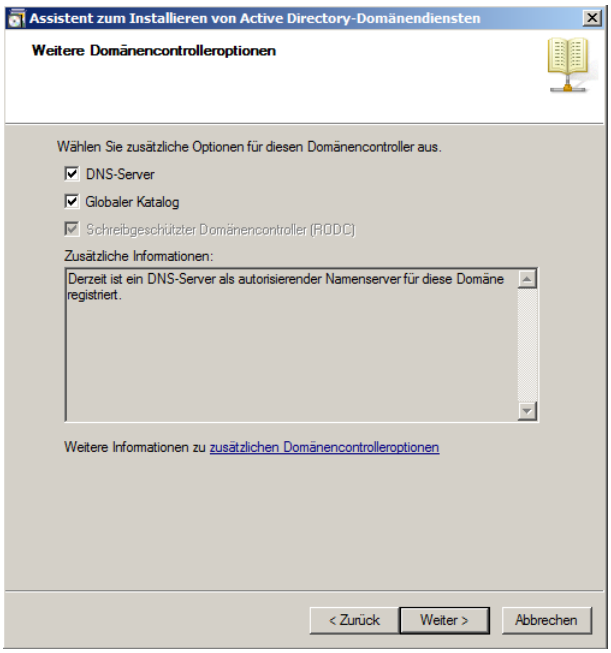
Im unteren Feld geben wir bei Abweichungen das Administratorkonto an.



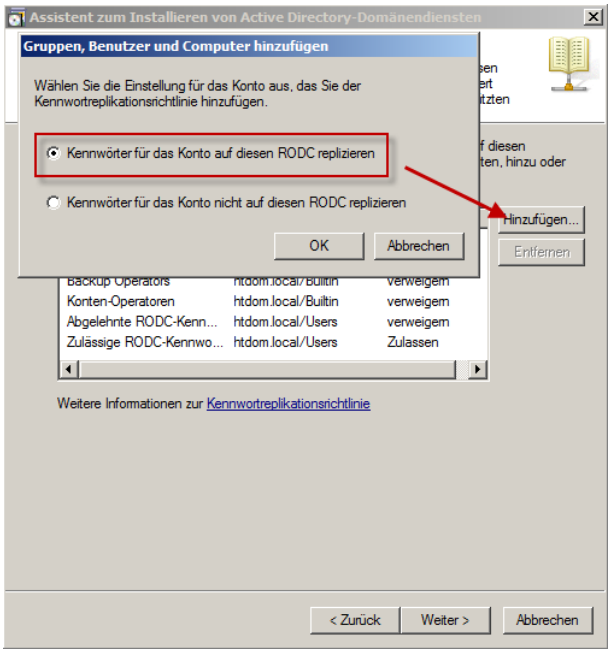
Im nächsten Fenster vergeben wir den Computernamen des RODC Servers.



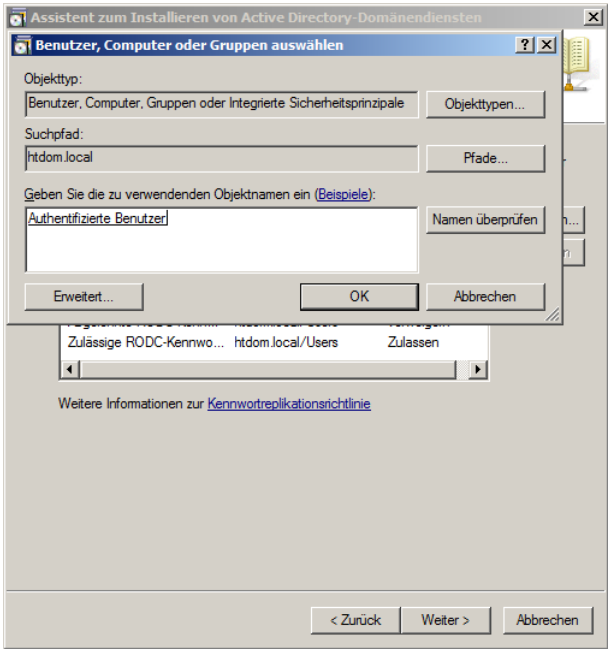
Wählen unsere Domain Site aus und klicken auf Weiter

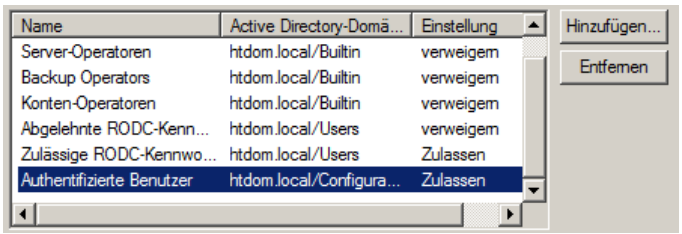


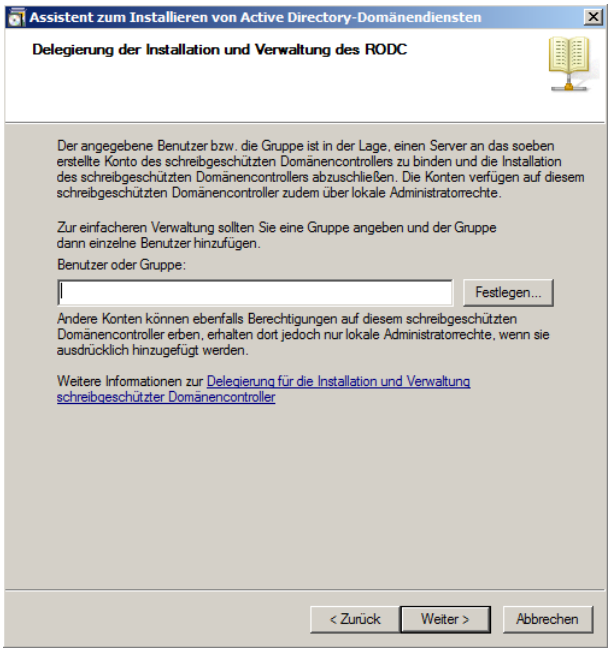
Wählen die Zusatzoptionen des Servers aus und klicken auf Weiter



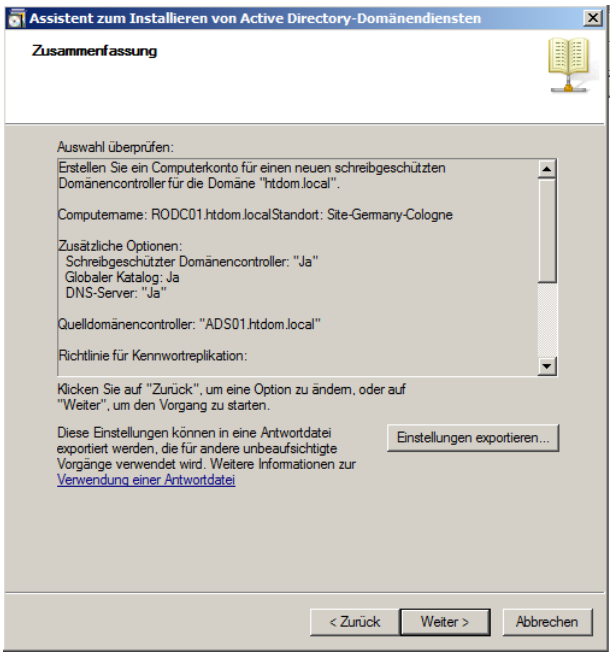
Im nächsten Fenster fügen wir die Gruppe Administratoren (Deny) und Authentifizierte Benutzer (Allow) hinzu.



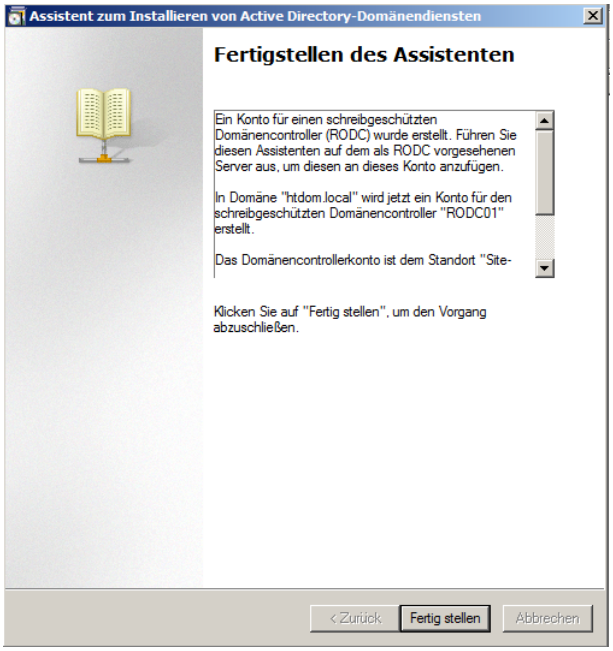




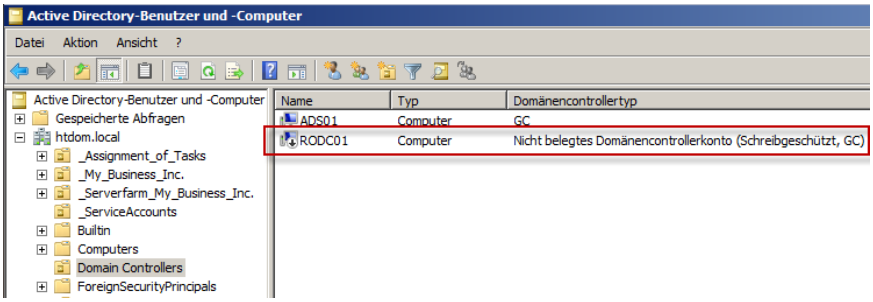
In diesem Fenster können wir noch spezielle Gruppen definieren die erhöhte Berechtigungen auf den RODC haben. → Leer lassen und auf Weiter klicken



Die Zusammenfassung bestätigen wir mit Weiter



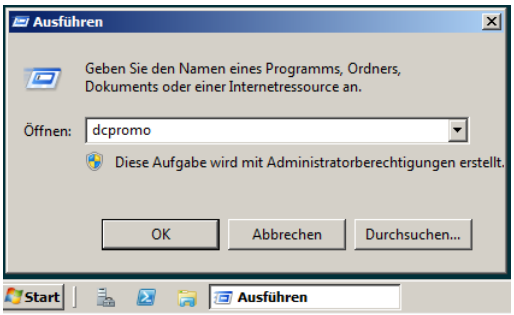
Und das letzte Fenster bestätigen wir mit Fertigstellen.



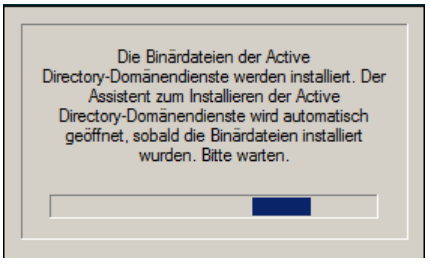
Nun sehen wir in der Oberfläche unserer Active Directory Benutzer und Computer Verwaltung das vorbereitete RODC Computer Konto.

Read Only Domain Controller - Bereitstellen

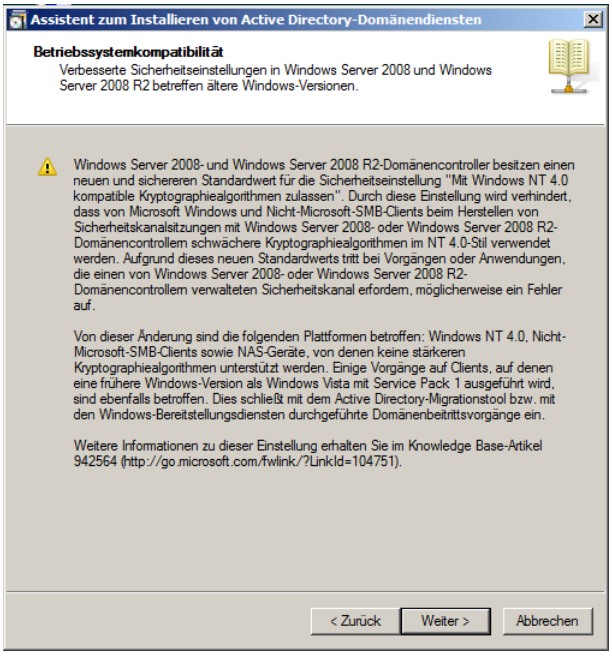
Im nächsten Schritt installiere ich einen neuen Windows Server 2008 R2 Server für den Außenstandort Köln mit den Computernamen RODC01.htdom.local, nach getaner Arbeit starte ich auch schon über Start → Ausführen den ***dcpromo***



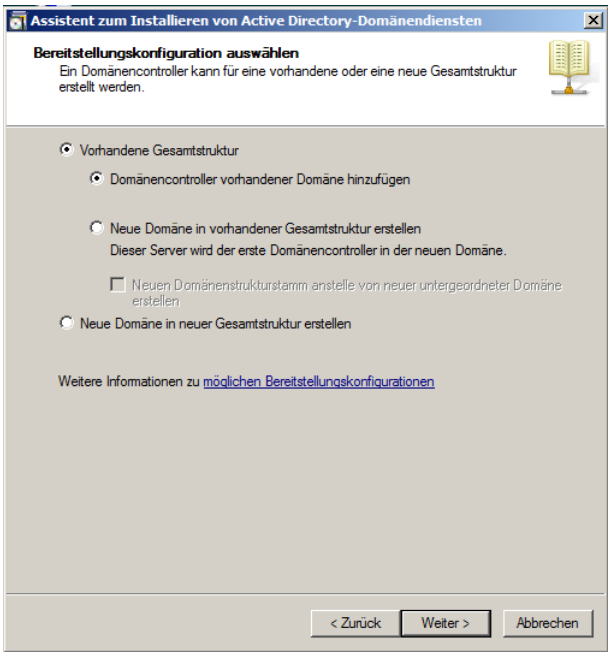
Die Binärdateien der Domänen Dienste werden installiert



Nach kurzer Zeit startet der Wizard für die Active Directory Einrichtung, hier schalten wir wieder den erweiterten Modus ein und klicken auf Weiter.

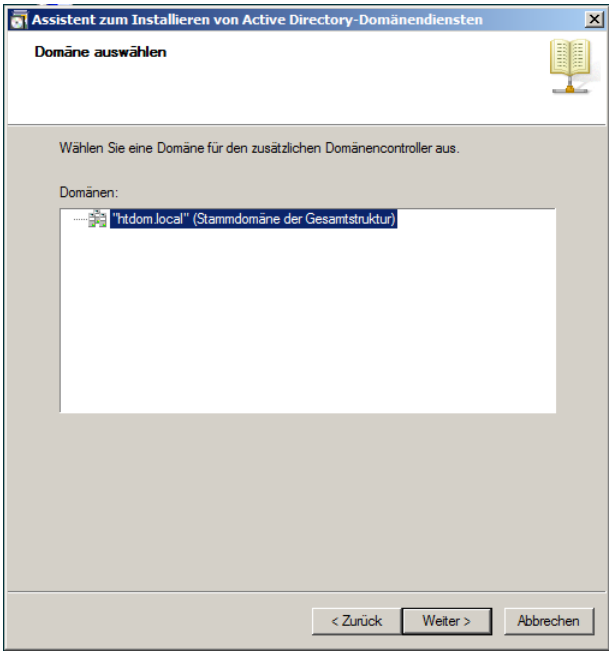


Das Fenster mit der Betriebssystemkompatibilität bestätigen wir wieder mit Weiter.

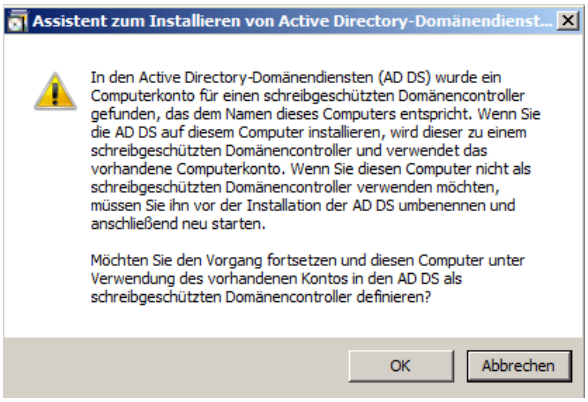


Im nächsten Fenster füge ich den Domain Controller einer bestehenden Domäne hinzu und klicke auf Weiter.

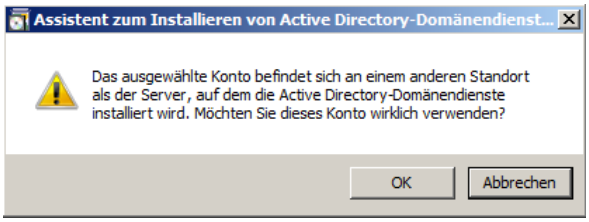
Im oberen Feld geben wir den Domänennamen an in der der RODC beitreten soll, im unteren Feld bei Abweichung das Administrator Konto.



Im nächsten fester bestätige ich die Domänenauswahl mit Weiter.



Jetzt werde ich von Microsoft darauf hingewiesen das es bereits ein Domänenkonto mit dem selben Namen gibt und ob das so in Ordnung ist, das bestätige ich mit OK.

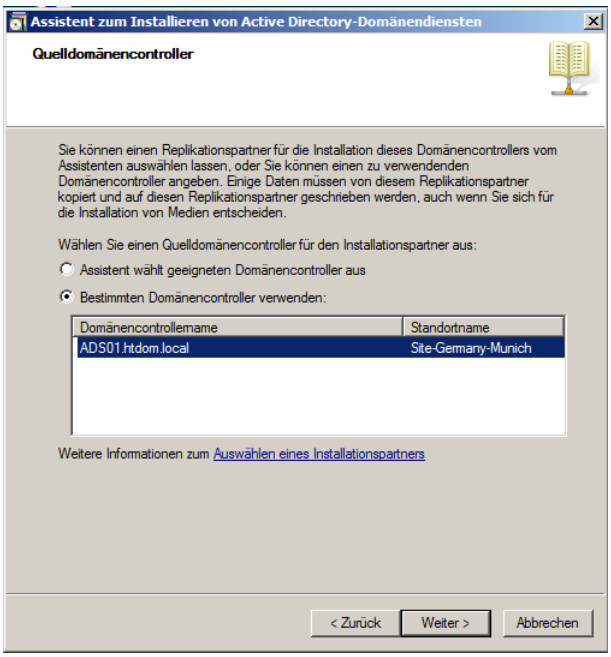


Und in der nächsten Meldung, werde ich darauf hingewiesen, das sich das Computerkonto in einer anderen DomainSite befindet, auch das bestätige ich mit OK.

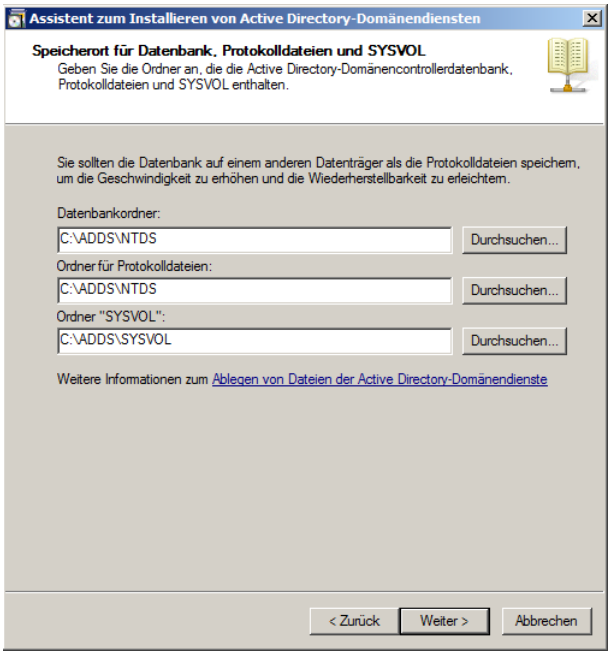
Die Active Directory Datenbank lasse ich über das Netzwerk replizieren, den unteren Punkt habe ich wenn ich ehrlich bin noch gar nicht ausprobiert, reiche ich bei Gelegenheit in diesem Howto nach.

Microsoft schreibt aber folgendes: Installieren eines RODC von einem Medium

http://technet.microsoft.com/de-de/library/cc754629%28WS.10%29.aspx#bkmk_instRODCmed

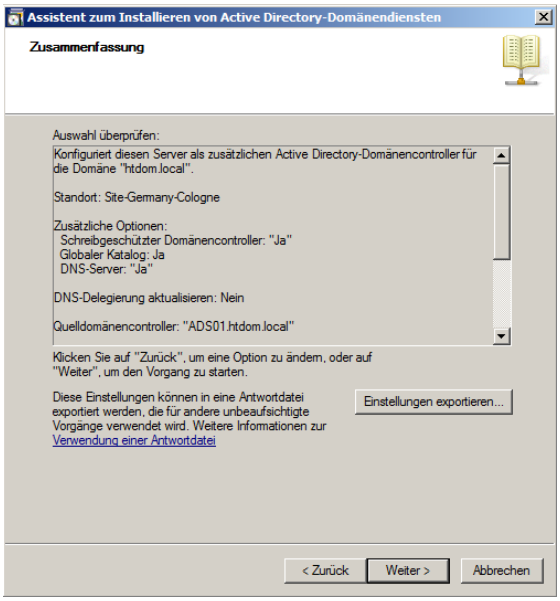


In diesem Fenster wähle ich den beschreibbaren Domänencontroller aus mit dem die Replizierung stattfindet.



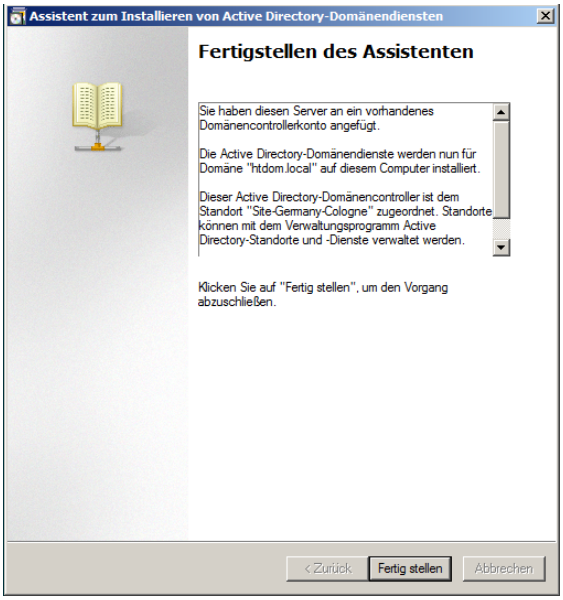
Wähle mir ein passendes Verzeichnis aus wo die Daten hin gespeichert werden.

Vergebe ein Passwort für den Wiederherstellungsmodus und klicke auf Weiter.

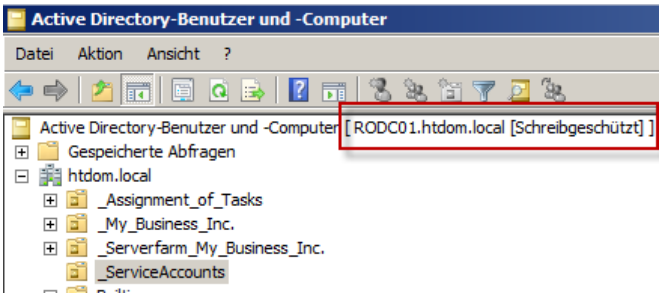


Die Zusammenfassung bestätige ich ebenfalls mit Weiter

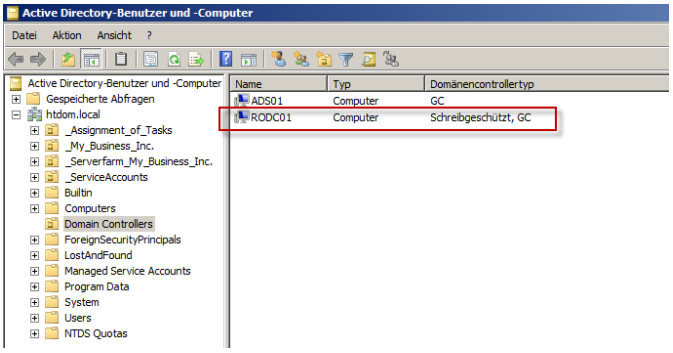
Ab jetzt wird Active Directory auf dem Server eingerichtet.



Wenn alles fertig ist schließe ich den Assistenten mit Fertigstellen und starte den Server einmal durch.



Wenn man nun die Verwaltungskonsole ***Active Directory Benutzer und Computer*** öffnet und sich mit den RODC verbindet sieht man dass dieser Schreibgeschützt ist.



Auf den beschreibbaren Domain Controller ist nun das Computerkonto von dem RODC aktive und im Replikation mit aufgenommen, Ab jetzt können wir den Domain Controller ausliefern und aufstellen.

Viel Spaß

Gruß Helmut Thurnhofer